(12)特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2002 年12 月5 日 (05.12.2002)

PCT

(10) 国際公開番号
WO 02/098065 A1

(51) 国際特許分類[7]: H04L 12/40, G05B 19/05

(21) 国際出願番号: PCT/JP02/05389

(22) 国際出願日: 2002 年5 月31 日 (31.05.2002)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願2001-164564 2001 年5 月31 日 (31.05.2001) JP

(71) 出願人 (米国を除く全ての指定国について): オムロン株式会社 (OMRON CORPORATION) [JP/JP]; 〒600-8530 京都府 京都市 下京区塩小路通堀川東入南不動堂町801 番地 Kyoto (JP).

(72) 発明者; および
(75) 発明者/出願人 (米国についてのみ): 宗田 靖男 (MUNETA,Yasuo) [JP/JP]; 〒600-8530 京都府 京都市 下京区塩小路通堀川東入南不動堂町801 番地 オムロン株式会社内 Kyoto (JP). 中村 敏之 (NAKAMURA,Toshiyuki) [JP/JP]; 〒600-8530 京都府 京都市 下京区塩小路通堀川東入南不動堂町801 番地 オムロン株式会社内 Kyoto (JP). 中山 晃行 (NAKAYAMA,Teruyuki) [JP/JP]; 〒600-8530 京都府 京都市 下京区塩小路通堀川東入南不動堂町801 番地 オムロン株式会社内 Kyoto (JP).

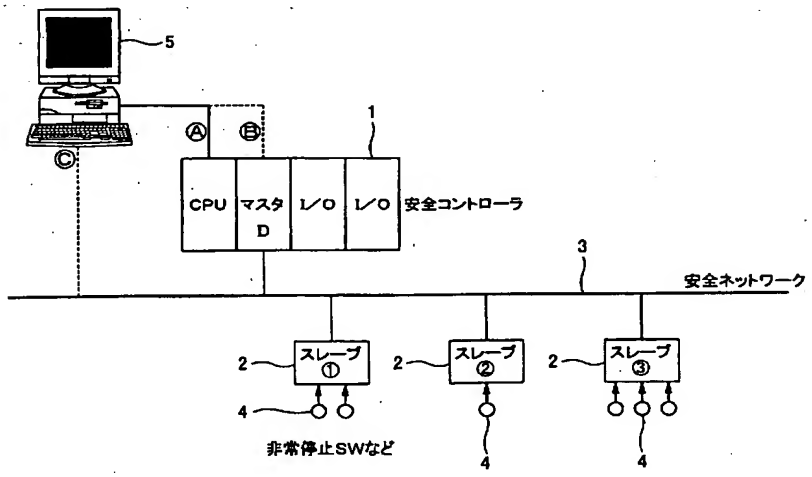
(74) 代理人: 松井 伸一 (MATSUI,Shinichi); 〒107-0052 東京都 港区 赤坂7丁目6番41号 赤坂七番館106 Tokyo (JP).

(81) 指定国 (国内): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZM, ZW.

[続葉有]

(54) Title: SAFETY NETWORK SYSTEM AND SAFETY SLAVES AND SAFETY CONTROLLER AND COMMUNICATION METHOD AND INFORMATION GATHERING METHOD AND MONITORING METHOD IN SAFETY NETWORK SYSTEM

(54) 発明の名称: 安全ネットワークシステム及び安全スレーブ並びに安全コントローラ及び通信方法並びに安全ネットワークシステムにおける情報収集方法及びモニタ方法



1...SAFETY CONTROLLER
3...SAFETY NETWORK
2...SLAVE (1), SLAVE (2), SLAVE (3) RESPECTIVELY
4...EMERGENCY STOP SW OR THE LIKE
D...MASTER

(57) Abstract: A safety PLC (1) and safety slaves (2) are connected via a safety network (3). Each safety slave has a safety information transmission function for transmitting safety information that specifies whether or not it is in a safe condition, and a non-safety information transmission function for transmitting non-safety information not including the safety information, and the non-safety information transmission function transmits non-safety information on condition that the relative safety slave is in a safe condition; it transmits safety information instead of non-safety information when safety is not judged at a non-safety information transmitting

[続葉有]

WO 02/098065 A1

(84) 指定国 (広域): ARIPO 特許 (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア特許 (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ特許 (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI 特許 (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:
— 国際調査報告書

２文字コード及び他の略語については、定期発行される各*PCT*ガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

timing. A safety controller, on receiving non-safety information, assumes a safety slave that has transmitted the non-safety information is in a safe condition.

(57) 要約:

安全ＰＬＣ１と、安全スレーブ２とが安全ネットワーク３を介して接続される。安全スレーブは、安全状態にあるか否かを特定する安全情報を送信する安全情報送信機能と、前記安全情報を含まない非安全情報を送信する非安全情報送信機能を有し、前記非安全情報送信機能は、前記安全スレーブが安全状態であることを条件に非安全情報を送信する。つまり、非安全情報を送信するタイミングの際に安全でないと判断した場合には、非安全情報を送ることなく安全を送信する。安全コントローラは、非安全情報を受信した場合には、その非安全情報の送信元の安全スレーブは安全状態にあると推定する。

明 細 書

安全ネットワークシステム及び安全スレーブ並びに安全コントローラ及び通信方法並びに安全ネットワークシステムにおける情報収集方法及びモニタ方法

技術分野

この発明は、安全ネットワークシステム及び安全スレーブ並びに安全コントローラ及び通信方法並びに安全ネットワークシステムにおける情報収集方法及びモニタ方法に関するものである。

背景技術

ファクトリーオートメーション（以下、「ＦＡ」と称する）で用いられるプログラマブルコントローラ（以下、「ＰＬＣ」と称する）は、スイッチやセンサなどの入力機器からＯＮ／ＯＦＦ情報を入力し、ラダー言語などで書かれたシーケンスプログラム（ユーザプログラムとも称する）に沿って論理演算を実行し、求められた演算結果に従い、リレーやバルブ，アクチュエータなどの出力機器にＯＮ／ＯＦＦ情報の信号を出力することで制御が実行される。

ところで、ＰＬＣと、入力機器並びに出力機器との接続形態は、ＰＬＣに直接接続する場合もあれば、ネットワークを介して接続する場合もある。係るネットワークで接続されたネットワークシステムを構築した場合、上記ＯＮ／ＯＦＦ情報の送受をネットワークを経由して行うことになる。このとき、通常、ＰＬＣ側がマスタとなり、機器側がスレーブとなるマスタスレーブ方式で情報の伝送が行われる。

一方、最近ではＰＬＣによる制御においても、フェイルセーフ（安全）システムが導入されつつある。つまり、ＰＬＣや各機器自体はもちろんネットワークも安全機能を組み込まれたもので構成される。ここで安全機能とは、安全であることを確認し、出力を行う機能である。そして、安全システムは、緊急停止スイッチが押下されたり、ライトカーテンなどのセンサが人（身体の一部）の進入を検出した場合等のネットワークシステムが危険状態になった場合に、フェイルセー

フが働き、システムが安全側になって、動作が停止するようにするものである。換言すると、上記した安全機能により、安全であることが格納されたときのみ出力し、機械を動かすシステムである。よって、安全が確認できない場合には、機械が停止する。

上記した安全機能を備えたネットワークシステム（安全ネットワークシステム）の場合、異常，危険状態その他の安全でない状態が発生した時から、安全動作（装置の停止等）を実行するまでに要する最大応答時間を一定にする必要がある。すなわち、良く知られているように、マスタースレーブ方式で情報伝送をする場合、図１（ａ）に示すように、マスタからの要求に従って各スレーブが順にマスタに安全応答を返すようになる。図示の例では、ネットワークシステムを構成するスレーブは３つある。なお、ここで扱うＯＮ／ＯＦＦ情報は、正常（安全）／異常（危険）という安全制御用のＩ／Ｏ情報である。最大応答時間は、１回の通信サイクルにかかる時間が保証される。

一方、定期的或いは非定期的に、上記安全情報以外のスレーブの状態や通電時間や動作回数などのスレーブ並びにスレーブに接続された機器を監視するための補完的な情報（非安全情報）を収集したいという要求がある。係る非安全情報を取得することにより、例えば機器の寿命判定が行え、実際に故障を生じてシステムが停止する前に交換することができる。

しかし、上記のように、非安全情報を送る場合、例えば図１（ａ）に示す例において通信サイクル１では全て非安全情報を送信し、次の通信サイクル２では全て安全情報を送信することが考えられる。しかし、係る方式によると、通信サイクル１の期間は安全情報を送ることができないので、結局最大応答時間は通信サイクルの２倍の長さとなる。

また、別の方式としては、図１（ｂ）に示すように、マスタからの要求に対し、安全情報を送信する安全応答に非安全情報を付加した情報を返すこともできる。この場合でも、図１（ａ）に示す安全応答のみ返す場合に比べると、１回の通信サイクルに要する時間が長くなる。従って、いずれの方式をとっても、最大応答時間を短くしたいという要求を満足することができなかった。

この発明は、システム稼働中に安全信号以外の情報をネットワークを介して送

受信しても、本来の安全信号の応答時間が遅れることの無い安全ネットワークシステム及び安全スレーブ並びに安全コントローラ及び通信方法並びに安全ネットワークシステムにおける情報収集方法及びモニタ方法を提供することを目的とする。

発明の開示

上記した目的を達成するため、この発明による安全ネットワークシステムは、安全コントローラと、安全スレーブとが安全ネットワークを介して接続されて構築される。ここで、安全ネットワークシステムとは、ネットワークシステム内において異常・危険など安全状態でなくなった場合に、フェイルセーフ機能が働き、異常・危険回避をすることができるものである。そして、安全コントローラ，安全スレーブ並びに安全ネットワークは、それぞれフェイルセーフ処理に対応する装置類である。

そして、前記安全スレーブは、安全状態にあるか否かを特定する安全情報を送信する安全情報送信機能と、前記安全情報を含まない非安全情報を送信する非安全情報送信機能を有し、前記非安全情報送信機能は、前記安全スレーブが安全状態であることを条件に非安全情報を送信するように構成した。

そして、好ましくは、前記安全スレーブは、前記非安全情報を送信するタイミングの際に安全でないと判断した場合には、前記非安全情報を送ることなく前記安全を送信する機能を設けることである。

また、この発明による通信方法は、安全コントローラと、安全スレーブとが安全ネットワークを介して接続されて構築される安全ネットワークシステムにおける通信方法であって、前記安全スレーブは、所定のタイミングで前記安全ネットワークを介して前記安全コントローラに向けて、安全状態にあるか否かを特定する安全情報と、前記安全情報を含まない非安全情報のいずれかの情報を送信する処理を行う。このとき、前記非安全情報を送信する処理は、前記安全スレーブが安全状態であることを条件に行う。

また、本発明に係る安全スレーブでは、安全状態にあるか否かを特定する安全情報を送信する安全情報送信機能と、前記安全情報を含まない非安全情報を送信

する非安全情報送信機能を有し、前記非安全情報送信機能は、安全状態であることを条件に非安全情報を送信するように構成した。ここで、安全スレーブにおける各送信機能は、実施の形態ではＭＰＵ２３により実現されている。

さらにまた、本発明に係る安全コントローラでは、前記安全スレーブから受信した安全情報の内容を解析し、安全状態に無いと判断した場合に所定の処理を実行するフェイルセーフ処理機能と、前記非安全情報を受信した場合には、送信元の前記安全スレーブは安全状態にあると推定する機能を備えることである。

本発明によれば、非安全情報が送信されるということは、安全スレーブの安全が保障されることを意味する。従って、安全スレーブが安全状態である場合には、安全コントローラは、安全情報を受信することにより安全スレーブが安全状態にあることを直接確認できる。そして、非安全情報を受信することにより間接的に安全スレーブが安全状態にあることを確認できる。また、仮に非安全状態を送信するタイミングのときに安全状態でなくなると、安全でないと言う安全情報（危険・異常）を送信するので、安全状態でなくなった場合にフェイルセーフが起動するまでの応答時間は、延ばさずに済む。

つまり、ユーザが必要とする非安全情報の更新時間を設定することができる。そして、非安全情報を送信したとしても安全状態が保障されているので、毎回安全情報を送信する場合に比べ、応答時間が長くならない。

換言すると、安全ネットワークのトラフィックに影響を与えず、非安全情報をスレーブ（安全スレーブ）からマスタ（安全コントローラ）に通知できる。よって、非安全情報の更新時間をユーザが設定できるので、ユーザアプリに合わせた管理が可能となる。また、システムを停止することなく、非安全情報の収集が可能なため、機器のモニタがオンラインで可能となる。

また、非安全情報の送信タイミングを制御するのは、安全コントローラ側と安全スレーブ側の何れでも良い。具体的には、前者の場合には、例えば、安全コントローラに、非安全情報の送信要求を発するタイミングを制御する非安全情報要求制御手段を設けることにより実現できる。この場合に対応する安全スレーブとしては、受信した前記安全コントローラからの要求が、安全情報の要求か非安全情報の要求かを判断し、前記安全情報の要求の場合には、安全情報を送信し、前

記非安全情報の要求の場合には、自己が安全状態にあるときは前記非安全情報を送信し、安全状態にないときは安全情報を送信するように構成することである。一方、後者の場合には、安全スレーブに、非安全情報を送信する送信タイミングを制御する非安全情報送信制御手段を設け、前記送信タイミングの際に、安全状態にあることを条件に前記非安全情報を送信するように構成することである。また、送信タイミングをいくつにするかの設定は、製造時にメーカが設定していても良いし、ユーザが設定できるようにしても良い。

安全情報とは、少なくも安全スレーブ及びまたはそれに接続された安全機器の状態が安全状態か否かの情報を含むものである。もちろん、それ以外の情報を含むことはかまわない。これに対し、非安全情報は、上記安全情報を含まない各種の情報であり、例えば、リレーの寿命，調査結果，通電時間，動作回数，型情報等がある。ここで、「通電時間」や「動作回数」などは、例えば、それぞれタイマやカウンタで計時・計数して求め、求めた現時点の数値を非安全情報として送る。また、「リレーの寿命」とは寿命予知である。つまり、ここでいう非安全情報としてのリレーの寿命は、寿命が来て安全動作ができない旨の情報ではなく（この時は安全情報扱いとなる）、安全に動作するがメンテナンス（交換，調整手入れなど）をする時期が近づいてきている旨の予知的な情報である。「調査結果」は、たとえば統計的に予知或いは検出するような旨の情報である。つまり、スレーブ側で安全かどうかを自己診断した結果ではない。この自己診断結果は安全情報として送られる。なお、非安全情報としての検査結果の例としては、安全に動作するが、①もう少しで寿命が来そうだとか、②悪い環境で使用されているとか、③温度④振動状態⑤供給電圧⑥酷使状態かどうか…などの情報がある。係る情報を知ることで、早めにメンテナンス（交換，調整手入れなど）をすることができ、寿命が来て動かなくなり、異常の影響が大きくなることが防止できる。

さらに本発明に係る安全ネットワークシステムにおける情報収集方法は、安全コントローラと、安全スレーブとが安全ネットワークを介して接続されて構築される安全ネットワークシステムを前提とする。そして、前記安全スレーブは、安全状態にあるか否かを特定する安全情報を送信する安全情報送信機能と、前記安全情報を含まない非安全情報を送信する非安全情報送信機能を有し、前記非安全

情報送信機能は、前記安全スレーブが安全状態であることを条件に非安全情報を送信するものであり、前記安全スレーブが、前記安全コントローラに向けて情報を送信するに際し、前記安全情報と前記非安全情報のいずれを送信するかを決定し、次いで、その決定した情報を前記安全ネットワークを介して送信し、前記安全コントローラは、前記安全ネットワークを介して送られてきた前記安全情報或いは前記非安全情報を受信し、受信した情報が前記非安全情報の場合に、その非安全情報に基づく情報を記憶する。

このようにすると、安全コントローラは、安全ネットワークに接続された安全スレーブから非安全情報を取得することができる。しかも、本来非安全情報の送信タイミングの時に安全でない場合には、安全情報が送られてくるので、安全システムとしての信頼性を低下することなく、非安全情報の収集ができる。また、非安全情報を収集した場合には、安全であることも間接的に認識できる。

また、本発明のモニタ方法は、安全コントローラと、安全スレーブとが安全ネットワークを介して接続されて構築される安全ネットワークシステムに対し、モニタ装置をさらに接続して構築されるシステムにおけるモニタ方法である。そして、前記安全スレーブは、安全状態にあるか否かを特定する安全情報を送信する安全情報送信機能と、前記安全情報を含まない非安全情報を送信する非安全情報送信機能を有するとともに、前記非安全情報送信機能は、前記安全スレーブが安全状態であることを条件に非安全情報を送信するものであり、前記モニタ装置は、前記安全スレーブから前記安全コントローラに向けて送信される前記非安全情報を取得し、その取得した非安全情報を解析し、その非安全情報に基づく情報を記憶するようにした。

ここで、モニタ装置は、安全コントローラに接続され、非安全情報は、その安全コントローラ経由で間接的に取得することができる。また、モニタ装置を安全ネットワークに接続し、安全ネットワーク上を伝送されるフレームを監視し、安全コントローラ宛の非安全情報をモニタ装置も受信することにより非安全情報を直接的に収集することもできる。

モニタ装置は、安全ネットワークに接続された安全スレーブから非安全情報を取得することができる。しかも、本来非安全情報の送信タイミングの時に安全で

ない場合には、安全情報が送られてくるので、安全システムとしての信頼性を低下することなく、非安全情報を収集し、モニタリングすることができる。なお、データの記憶方法としては、ロギングデータその他各種の形式で保存することができる。しかも、非安全情報を取得した場合には、安全システムは、安全状態にあることを間接的に認識できる。なお、このモニタ装置は、実施の形態では、パソコン５によるツールに対応する。また、モニタリング装置や、コンフィグレータなどと称されるものも、このモニタ装置に対応する。

図面の簡単な説明

図１は、従来例を示す図である。

図２は、本発明に係る安全ネットワークシステムの好適な一実施の形態を示す図である。

図３は、本発明に係る安全コントローラ（ＰＬＣ）の好適な一実施の形態の要部を示す図である。

図４は、本発明に係る安全スレーブの好適な一実施の形態を示す図である。

図５は、本実施の形態の作用を説明する図である。

図６は、送信フレームのデータ構造の一例を示す図である。

図７は、安全ＰＬＣ（マスタユニット）のＭＰＵの機能を説明するフローチャートの一部である。

図８は、安全ＰＬＣ（マスタユニット）のＭＰＵの機能を説明するフローチャートの一部である。

図９は、安全ＰＬＣ（マスタユニット）のＭＰＵの機能を説明するフローチャートの一部である。

図１０は、安全スレーブのＭＰＵの機能を説明するフローチャートである。

図１１は、本実施の形態の作用を説明する図である。

図１２は．別の実施の形態の作用を説明する図である。

図１３は、変形例の作用を説明する図である。

図１４は、変形例の安全スレーブのＭＰＵの機能を説明するフローチャートである。

図１５は、変形例における送信フレームのデータ構造の一例を示す図である。

図１６は、変形例における情報受信側の機能を説明するフローチャートの一部である。

発明を実施するための最良の形態

本発明をより詳細に説明するにあたり、添付の図面に従ってこれを説明する。具体的には、図２は、本発明が適用される安全ネットワークシステムの一例を示している。図２に示すように、安全ＰＬＣ１と複数の安全スレーブ２が安全ネットワーク３を介して接続されている。各安全スレーブ２には、非常停止スイッチなどの他、各種の入力機器や出力機器等の各種安全機器４が接続されている。安全ＰＬＣ１は、ＣＰＵユニット１ａ，マスタユニット（通信ユニット）１ｂ，Ｉ／Ｏユニット１ｃなどの複数のユニットを連結して構成されている。

更に、ツールとしてのパソコン５が、安全ＰＬＣ１のＣＰＵユニット１ａやマスタユニット１ｂ並びに安全ネットワーク３に接続可能となっている。このパソコン５は、安全ＰＬＣ１を介して安全スレーブ２、ひいてはそれに接続された安全機器４についての情報を収集し、管理する。

この安全ネットワークシステムを構成する各種装置は、全て安全機能（フェイルセーフ）が組み込まれたものを用いている。この安全機能は、安全であることを確認し、出力（制御）を行う機能である。そして危険状態になった場合にフェイルセーフが働いて、システムが安全側になって動作を停止させる。つまり、安全システムは、緊急停止スイッチが押下されたり、ライトカーテンなどのセンサが人（身体の一部）の進入を検出した場合等のネットワークシステムが危険状態になった場合に、フェイルセーフが働き、システムが安全側になって、動作が停止するようにするものである。換言すると、上記した安全機能により、安全であることが格納されたときのみ出力し、機械を動かすシステムである。よって、安全が確認できない場合には、機械が停止する。

次に、このような安全機能のうち、本発明の要部となる情報の送受について説明する。マスタユニット１ｂには、通信機能も組み込まれており、安全スレーブ２との間でマスタ・スレーブ方式で情報の送受を行うようになっている。基本的

には従来と同様で、図１（ａ）に示すように安全ＰＬＣ１（マスタユニット１ｂ）からの要求に従い、その要求を受けた安全スレーブ２は、安全応答として安全情報を返す。安全スレーブ２に対し、①→②→③といように順番に要求を発し、３つ全ての安全スレーブ２から安全情報を収集することを１つの通信サイクルとし、その通信サイクルを繰り返し実行する。

そして、上記通信の制御を行うマスタユニット１ｂは、図３に示すような内部構造をとっている。すなわち、システムＲＯＭ１１に格納されたプログラムを読み出し、システムＲＡＭ１２のメモリ領域を適宜使用して所定の処理を実行するＭＰＵ１０を有し、更に、安全ネットワーク３と接続され、所定の安全スレーブ２との間でデータの送受を行うための通信インタフェース１３を備えている。更にまた、安全スレーブ２から送られてきた非安全情報を記憶する非安全情報記憶部１４を備えている。すなわち、本実施の形態でも、従来と同様に各安全スレーブ２から、非安全情報が送られてくるので、受信した非安全情報を安全スレーブのアドレスに関連づけて記憶する。この非安全情報記憶部１４に記憶された安全スレーブの非安全情報は、定期的或いはパソコン（ツール）５の読み出し命令に従い抽出される。

なお、当然のことながら、このマスタユニット１ｂも安全ネットワークシステムに対応しているものであるので、各種の安全機能が組み込まれている。すなわち、図示は省略するが、例えばＭＰＵ１０を２個設け、同時に同一プログラムを実行させ、その結果が一致したときのみ正しい出力として処理する機能を設ける。もちろん、安全ネットワークシステムに対応するためのこれ以外の安全機能も具備する。

そして、マスタユニット１ｂのＭＰＵ１０で実行するプログラムの一例としては、例えば、上記した所定の安全スレーブ２に対して要求を発信し、その要求に対する応答を受信するとともに、受信した応答内容に従い所定の処理を実行するものである。もちろん、ＣＰＵユニット１ａからの命令に従い、所定の安全スレーブ２に対して情報を送信する処理もある。

一方、安全スレーブ２の内部構造は、図４に示すようになっている。同図に示すように、安全ネットワーク３に接続し、安全ＰＬＣ１（マスタユニット１ｂ）

との間でデータの送受を行う通信インタフェース２１と、安全スレーブ２に接続された安全機器４との間でデータの送受を行うための入出力インタフェース２２と、システムＲＯＭ２４に格納されたプログラムを読み出し、システムＲＡＭ２５のメモリ領域を適宜使用して所定の処理を実行するＭＰＵ２３を備えている。ＭＰＵ２３は、通信インタフェース２１を介して受信した自己宛の要求に従い、入出力インタフェース２２を介して安全機器４から取得した情報（安全情報等）を、通信インタフェース２１，安全ネットワーク３を経由してマスタユニット１ｂに返す処理を行う。

さらに、ＭＰＵ２３は、自己診断機能や、安全機器４の動作状態（通電時間，ＯＮ／ＯＦＦ回数など）監視機能を備え、各機能を稼働させて得られた診断結果や動作状態などの非安全情報を非安全情報格納用メモリ２６に格納する処理も実行する。そして、この非安全情報格納用メモリ２６に格納された非安全情報も、マスタユニット１ｂからの要求に従い返送することにより、マスタユニット１ｂに非安全情報を伝達するようになっている。

つまり、マスタユニット１ｂからの要求は、安全情報の要求と非安全要求の情報の２種類があり、安全スレーブ２は、要求された種類の情報を応答として返す。なお、実際には、送信する都度１ずつインクリメントするシーケンスＮｏを付加した要求を行い、そのシーケンスＮｏの値によって各安全スレーブは安全情報と非安全情報のどちらの要求かを判断するようにしている。

ここで本実施の形態では、マスタユニット１ｂに非安全情報要求制御部１５を設け、各安全スレーブ２から非安全情報を収集するタイミングを任意に設定し、実行するようにしている。すなわち、非安全情報要求制御部１５は、タイマ或いはカウンタなどからなり、一定時間経過する毎、或いは通信サイクルが一定回数行われる毎にトリガ信号をＭＰＵ１０に送る。ＭＰＵ１０は、通常状態では安全情報取得のための要求を行い、前記トリガ信号を受信した場合には、その次の１サイクルは非安全情報の取得のための要求を行うようにする。このようにすると、ユーザが設定したサイクルで非安全情報を収集することができる。もちろん、システムの稼働中でも行える。なお、この要求の出力についてのＭＰＵ１０の詳細な処理機能の説明は後述する。

一方、安全スレーブ２は、上記した通り、マスタユニット１ｂからの要求に伴い安全情報または非安全情報のいずれかを返す。このとき、安全スレーブ２は、さらに以下のような処理を行う。つまり、安全情報の要求の場合には、そのままそのときの安全情報を返す。非安全情報の要求の場合には、まず、その安全スレーブ２が安全状態であるか否かを判断し、安全状態の場合には非安全情報を返し、安全状態でない場合（危険，異常）には、安全情報を送信する。すると、この場合の安全情報は「異常通知」を意味する。

このようにすると、非安全情報が送られてきた場合には、その非安全情報を送ってきた安全スレーブ２は安全状態にあることが保証される。よって、マスタユニット１ｂでは、非安全情報の要求に伴い安全スレーブ２から非安全情報の応答があった場合には、安全であるとみなせるので緊急停止などのフェイルセーフの処理をする必要が無く、当初の目的である非安全情報を所定の間隔で収集できる。また、安全スレーブ２が安全状態にない場合には、たとえ非安全情報の要求をした場合でも安全情報（異常通知）が送られてくるので、それに伴い所定の安全処理を行う。従って、異常発生に伴う応答時間は、１回の通信サイクルに要する時間が保証できる。

一例を示すと、図５のようにＮ－１回目の通信サイクルでは通常の安全情報の要求を行い、Ｎ回目の通信サイクルで非安全情報の要求を行う場合を想定する。すると、各安全スレーブ２が安全状態にある場合には、図５（ａ）に示すように各安全スレーブからは、要求のあった種類の情報を返す。これに対し、例えば、安全スレーブ②がＮ－１回目の通信サイクルで安全応答を返した後で異常が発生した場合には、次のＮ回目の通信サイクルの安全スレーブ②は、安全応答を送るので、この異常発生から安全応答を出力するまでの時間ｔは、１回の通信サイクルの時間Ｔ０よりも短くなる。

なお、上記した処理を実現するためには、マスタユニット１ｂ側で受信した情報が安全情報なのか非安全情報なのかを識別する必要がある。そこで、本実施の形態では、送信フレームに格納する情報として、図６に示すように安全情報と非安全情報を識別するための識別ビットを付加するようにした。これにより、マスタユニット１ｂは、識別ビットの値を見ることにより、受信した送信フレームが

、安全情報か非安全情報かを判別できる。

次に、上記した一連のデータ通信を行うための安全ＰＬＣ１（マスタユニット１ｂ）のＭＰＵ１０と、安全スレーブ２のＭＰＵ２３にて実行される処理手順について説明する。マスタユニット１ｂのＭＰＵ１０は、図７から図９に示すフローチャートを実行する機能を有する。前提として、図１に示すように安全スレーブ２は、①から③の３個有し、非安全情報の更新周期は通信サイクル単位で行い、３回に１回の割合で取得するものとする。

電源が投入されると、ユーザからの非安全情報の更新周期の設定入力を待つ（ＳＴ１，ＳＴ２）。そして、非安全情報の更新周期（この例では通信サイクルが３回毎）が設定されると、シーケンスＮｏ．３を非安全にし（ＳＴ３）、各スレーブ（①から③）のシーケンスＮｏ．３に非安全情報を要求するように設定する（ＳＴ４，ＳＴ５）。本実施の形態では、上記した更新周期の設定を非安全情報要求制御部１５が行う。

もちろん、更新タイミングがＮ回に１回の割合とする場合には、ステップ３の非安全への変換は、シーケンスＮｏ．＝「Ｎ」を非安全に設定することになる。また、本形態では、非安全情報の収集を全ての安全スレーブに対して同一の通信サイクル（この例では３回目）で行うようにしたが、各安全スレーブ毎に設定し、異なる通信サイクルで収集するようにしてももちろん良い。さらには、各安全スレーブ毎に更新周期を変えることもできる。

上記した各処理が完了すると、実際に安全ネットワークシステムを稼働させ、所定の制御を行うようになる。すなわち、まず、シーケンスＮｏ．の値であるｎに１をセットし（ＳＴ６）、安全スレーブ①に対して要求を送信する（ＳＴ７）。この要求には、シーケンスＮｏ．を付加して行う。従って、電源投入後の最初の要求は、シーケンスＮｏ．＝「１」の要求となる。

そして、安全スレーブ①からの応答を待ち、当該安全スレーブ①からの送信フレームを受信したならば、識別ビットを解析し、値が「０」であるか否かを判断する（ＳＴ８）。識別ビットが「０」でない場合、つまり、「１」の場合には安全情報が送信されてきたので、そのデータ部を解析し、安全スレーブ①の安全情報を受信する（ＳＴ９）。そして、安全状態が「安全」か否かを判断し（ＳＴ１

0）、安全の場合には安全スレーブ②に対してシーケンスＮｏ．ｎを付加した要求を送信する。

一方、ステップ８の分岐判断でＹｅｓ、つまり識別ビットが０の場合には送られてきた情報は非安全情報であるので、ステップ１１に飛び、安全スレーブ①についての非安全情報を受信する（ＳＴ１１）。また、今回の安全スレーブ①の安全状態は安全と推定する（ＳＴ１２）。その後、ステップ１３に進みスレーブ②に要求を出力する。

上記と同様の処理を安全スレーブ②に対して行い（ＳＴ１３からＳＴ１８）、続いて安全スレーブ③に対して行う（ＳＴ１９からＳＴ２４）。これにより、１回の通信サイクルに伴い安全情報或いは非安全情報の収集が行える。

そして、３つの安全スレーブ①から③からの情報を取得したならば、ｎが３以上か否かを判断し（ＳＴ２５）、３未満の場合にはｎを１インクリメントし（ＳＴ２６）、３以上の場合にはｎ＝１にする（ＳＴ２７）。その後、ステップ７に戻り、次の通信サイクルを実行する。以後、上記したステップ７からステップ２８までの処理を繰り返し実行する。

また、ステップ１０，１６，２２の安全か否かの判断で、「Ｎｏ」、つまり受信した安全情報が「安全でない」場合には、ステップ２８に飛び、安全出力を遮断し、動作を停止する（ＳＴ２８，ＳＴ２９）。なお、係るステップ２８，２９における具体的な処理は、従来からある安全ネットワークシステムにおける異常通知（危険）に伴う処理と同様であるので、その詳細な説明を省略する。

一方、各安全スレーブのＭＰＵ２３の動作は、図１０に示すようになる。すなわち、電源投入後、マスタユニット１ｂから送られてくる非安全情報を送信するシーケンスＮｏ．を取得し、設定する。ここでは、シーケンスＮｏ．＝「３」が非安全情報を送信するタイミングであると設定する（ＳＴ３0，ＳＴ３１）。

次いで、マスタユニット１ｂからの要求を待ち（ＳＴ３２）、要求を受けると、現在安全状態か否かを判断する（ＳＴ３３）。そして、安全でない場合には、安全情報として「危険」を送信する（ＳＴ３４）。また、安全状態の場合には、要求とともに付加されてきたシーケンスＮｏ．をチェックし、Ｎｏ．が「３」の場合には非安全情報を送信し、３以外の場合には安全情報（安全）を送信する（

ＳＴ３５，３６，３７）。以後、上記したステップ３２からステップ３７までの処理を繰り返し実行する。

上記した処理を１つの安全スレーブの動きを基準に見ると、図１１に示すようになる。つまり、マスタユニット１ｂから送られてくる要求にはシーケンスＮｏ．が付加されており、その値は、「１→２→３→１…」というように１から３を順次繰り返した値となる。そして、シーケンスＮｏ．＝「３」の要求を受けた際に非安全情報を返す。これにより、図１１（ａ）に示すように、安全スレーブが安全状態にあるとすると、マスタ側ではその安全スレーブの非安全情報を３回に１回受信することになり、その非安全情報を受信することにより安全確認ができる。

また、図１１（ｂ）に示すように、シーケンスＮｏ．＝「３」のときに安全でなくなった場合には、非安全情報を送ることなく安全応答をする。従って、マスタ側では非安全情報は受信できないが、安全応答に基づき危険状態にあることがわかるので、停止処理など所定の安全処理を行う。なお、図示省略するが、シーケンスＮｏ．１，２の要求のときに安全でなくなった場合には、通常通り安全応答（異常通知）をするので、それに基づき所定の安全処理を行う。

なお、上記した実施の形態では、Ｎ回に１回の割合で非安全情報を取得するようにしたが、本発明はこれに限ることはなく、一定時間毎に非安全情報を取得するようにすることもできる。この場合は、上記したように非安全情報を送信するシーケンスＮｏ．を決めるのではなく、マスタが出す要求にフラグを付けるなどして、通常の安全情報の要求と、非安全情報の要求を安全スレーブ側で識別できるようにする。そして、非安全情報要求制御部１５は、タイマを持ち、設定された時間経過する都度、トリガ信号をＭＰＵ１０に送る。そして、ＭＰＵ１０は、通常は安全情報用の要求を出し、トリガ信号を受信した際に非安全情報用の要求を出すようにすることもできる。

また、通信サイクルの回数により非安全情報を収集する場合でも、例えば、上記のようにマスタが安全情報用の要求と、非安全情報用の要求を出力するような場合、非安全情報要求制御部１５がカウンタを備え、要求を出力した回数をカウントし、所定回数に達したならばトリガ信号を出力し、そのトリガ信号を受けた

ＭＰＵ１０が非安全情報用の要求を出力するようにすることもできる。

一方、上記した例では、マスタ側で非安全情報の取得タイミングを制御するようにしたが、本発明はこれに限ることはなく安全スレーブ側で制御することもできる。この場合に、図４に示すように、安全スレーブ２に、非安全情報送信制御部２８を設ける。この非安全情報送信制御部２８は、タイマ或いはカウンタなどからなり、予め設定した非安全情報の更新タイミング（一定時間，一定通信回数）になると、非安全情報送信用のトリガ信号をＭＰＵ２３に与える。

ＭＰＵ２３は、マスタユニット１ｂから要求があると、通常は安全応答をし、安全情報（安全／危険）を返す。そして、上記トリガ信号を受けた場合には、要求を受けると、現在の安全状態を確認し、安全状態にある場合には非安全情報を送る。但し、安全状態でない（異常，危険）場合には、トリガ信号を受けた場合でも安全応答をする。なお、ＭＰＵ２３は、安全情報と非安全情報のどちらの情報を送信したかがマスタユニット側でわかるようにするために、例えば本例でも図６に示すように送信フレーム中に認識ビットを設け、「０」または「１」をセットする。

一方、マスタユニット１ｂ側は、所定の通信サイクルで順次各安全スレーブに対して要求を送信し、対応する安全スレーブからの応答を待つ。そして、安全スレーブからの送信フレームを受信すると、認識ビットを確認し、安全情報と非安全情報のどちらの情報かを識別する。そして、非安全情報の場合には、取得した非安全情報を非安全情報記憶部１４に格納するとともに、安全であることを認識する。また、受信した情報が安全情報の場合には、その内容を取得し、安全でない場合には、所定の安全処理を実行する。

このときのマスタースレーブ間でのデータの送受信のタイミングチャートを示すと、図１２のようになる。そして、図示の例では、各安全スレーブがいずれも安全状態であったため、それぞれの非安全情報を送信するタイミングで非安全情報を送信し、これを受けたマスタは非安全情報を取得するとともに、安全であることが確認できる。そして、この非安全情報を送信するタイミングのときに安全でない場合には安全応答をすることになる。また、各安全スレーブ側でそれぞれ送信タイミングを管理しているので、図示するように、必ずしも同一の通信サイ

クルのときに全ての安全スレーブから非安全情報が送られるとは限らない。

さらにまた、上記した実施の形態では、マスタからの要求に対して所望のスレーブがレスポンスを返すと行ったマスタースレーブ方式を説明した。すなわち、安全情報と非安全情報のいずれを送信するかの決定権は、マスタ側と安全スレーブ側のいずれでも良いことは、既に述べた通りであるが、いずれにしても、各スレーブからの送信タイミングは、マスタからのリクエストというように外部トリガに起因したものである。しかし、本発明で言うスレーブは、このようにマスタースレーブ間通信を行うものに限られない。つまり、スレーブとは称するものの、通信方式は任意のものを利用できる。その点では、厳密に言うと一般的に定義されているスレーブとは異なる概念を含むものであると言える。つまり、本発明で言う所のスレーブは、安全情報と非安全情報を適宜のタイミングで切替えながら送信する機能が有れば、実際に送受信する際の通信プロトコルは任意である。特に本発明で送信対象とする非安全情報の送信先は、マスタユニットやコントローラに限ることはなく、ネットワークに接続されたコンフィグレータ（コンフィグレーションツール）や、モニタリング装置や他のスレーブなど、自ノード以外のデバイス、つまり他ノードとすることができる。

そして、通信方式も、送信相手に応じて適宜選択できる。もちろん、送信するためのトリガも、上記したマスタからのリクエストのように外部からの要求に応じて行うものに限ることはなく、内部トリガ（内部のタイマ，一定の条件に合致したときに発生するイベントなど）に基づいて送信してもよい。

ここで、「内部トリガ」とは、スレーブ自身の所定の処理実行の結果に基づくもので、スレーブ内部で生成されるものである。そして、内部トリガの一例を示すと、スレーブで取得した非安全情報（入出力機器の状態情報等）が、予め設定した状態になった場合がある。つまり、例えば、入出力機器に対する通電時間が５０００時間を超えた場合に内部トリガを発生させたり、動作回数が１万回を越えた場合に内部トリガを発生させることである。また、スレーブ内に時計を持たせておき、その時計により所定時間経過のたびに周期的に内部トリガ信号を生成したり、所定時刻で内部トリガ信号を生成するものもある。

そして、予め設定した状態になった場合に内部トリガを発生させるようにする

と、その設定を適切に行なうことにより、頻繁に非安全情報を送ることを抑制し、通常の通信では、安全情報を送信することができる。そして、例えば入出力機器の動作状態に応じて定期的に、或いは、入出力機器が寿命に近づいてきたとき等に内部トリガを発生させて非安全情報を送信することにより、効率よく、必要な非安全情報を送信することができる。つまり、例えば動作回数や通電時間等の場合には、前回取得したデータから数回や数分程度変化したとしてもさほど重要性の高い情報ではない。そこで、係る重要性の高くない情報を送ることを抑制することにより、効率よく安全情報と非安全情報を送信することができる。

そして、係る内部トリガに基づいて安全スレーブ側から情報の発信をする場合のタイムチャートとしては、例えば図１３に示すようになる。すなわち、各送信デバイス（安全スレーブ）は、それぞれ内部タイマを持ち、送信タイマ間隔毎に内部トリガを発生する。この内部タイマを受けて、それぞれの安全スレーブは、安全奥羽等或いは非安全情報を所定の送信先に向けて出力する。この送信先は、予め設定しておくことにより、マスタや、他のスレーブなど、ネットワークに接続された他のノードに向けて送信することができる。

また、各安全スレーブは、自己の内部タイマに基づいて送信するが、既に他の安全スレーブが送信中の場合には、送信を停止し、同時に送信しようとしてネットワーク上で衝突した場合には、優先順位の高い安全スレーブ（ノード番号の小さいもの）側がそのまま通信を継続する。これにより、１回の通信サイクルで、所定の順で各安全スレーブから順次情報を送信することができる。そして、送信タイマを適宜に設定することにより、以後は、その順でスムーズに繰り返し情報の送信が行える。

そして、係る送信処理を行う安全スレーブ側のＭＰＵの機能としては、例えば図１４に示すフローチャートのようになる。この機能は、基本的には図１０に示した処理フローに対応するものである。つまり、まず電源ＯＮに伴い、非安全情報の送信シーケンスＮｏを設定する（ＳＴ４１）。この例では、全ての安全スレーブにおいて、送信シーケンスＮｏは「３」に設定するようにしているが、この数値は任意であり、安全スレーブ毎に替えてももちろん良い。

設定が完了したならば、送信条件、つまり、内部トリガが発生するのを待つ（

ＳＴ４２）。そして、内部トリガが発生すると、現在が安全か否かを判断し（ＳＴ４３）、安全でない場合には、安全情報（危険）を送信する（ＳＴ４４）。一方、安全の場合には、シーケンスＮｏを確認し（ＳＴ４５）、３未満の場合には、安全情報（安全）を送信するとともに、シーケンスＮｏであるＮを１インクリメントし（ＳＴ４６，ＳＴ４７）、ステップ４２に戻り次の送信条件に来るのを待つ。また、シーケンスＮｏが３以上の場合には、非安全情報送信タイミングであるので、非安全情報を送信する（ＳＴ４８）。その後、Ｎを１にセット後（ＳＴ４９）、ステップ４２に戻り次の送信条件に来るのを待つ。

なお、ステップ４５における判断のしきい値が「３」としているが、これはステップ４１にて非安全情報を送信するシーケンスＮｏの設定を「３」にしたためであり、ステップ４１における設定が３以外の場合には、このステップ４５における判断基準値もそれに合わせて変動する。

また、現在送信した情報が、安全情報であるのか、非安全情報であるのかは、送信フレー煙中に設定する識別ビット（図１５参照）により、特定する。従って、安全スレーブは、送信する際に、どちらの情報かに合わせて識別ビットを設定する。

一方、上記した安全スレーブからの情報を受信する側のデバイスとしては、図１６に示すフローチャートを実施する機能を有する。すなわち、まず、電源投入後、上記した安全スレーブから送られてくるフレームを受信するのを待つ（ＳＴ５１）。そして、受信したならば、それが正常受信か否かを判断し、異常の場合（ステップ５２でＮｏ）には、出力停止などの安全出力手段処理を行う（ＳＴ５７）。また、正常に受信した場合には、識別ビットを確認し、０の場合には、受信したデータは非安全情報であるので、非安全情報受信処理を行う（ＳＴ５４）。つまり、取得した非安全情報を所定エリアに格納したり、内容を解析し、解析結果に応じた処理を行う。その後、ステップ５１に戻り次の受信を待つ。

一方、識別ビットが１の場合には、安全情報であるので、安全情報受信処理を行い（ＳＴ５５）、通知内容が安全か否かを判断する（ＳＴ５６）。そして、安全の場合には、ステップ５１に戻り次の受信を待つ。また、通知内容が危険等の安全でない場合には、出力停止などの安全出力手段処理を行う（ＳＴ５７）。な

お、安全情報や非安全情報を受信した後の処理自体は、上記した実施の形態と同様であるので、詳細な説明を省略する。

また、識別ビットであるが、上記した説明では、安全情報と非安全情報を「1」と「0」の1ビットで示す場合を説明したが、本発明はこれに限ることはなく、さらに別の情報を付加することができる。つまり、非安全情報の場合には、データ部に格納する具体的な情報としては、スレーブに接続された入出力機器の通電或いは動作の積算時間や、動作回数等各種のものがあり、単に数値データのみ送信した場合では、何の情報を送ったかを認識できない場合がある。係る場合に、データ部の中身に応じて、非安全情報の種類等を特定する識別コードを付加すると良い。さらに、I／O端子は、複数個用意されている。従って、仮に8点あるとすると、8ビットの識別コードを用意し、各点毎に安全情報と非安全情報の識別ビットを立てるようにすることができる。また、係る場合、例えば、8点全てが非安全情報を送信したり、逆に安全情報を送信する場合には、8ビットを全て同一の識別ビットすることになるが、代表して1ビットにすることができる。これにより、送信データを圧縮し、短時間で送信可能となる。なお、係る場合には、圧縮している識別コードか圧縮していない識別コードかを識別するためのフラグが必要となる。

産業上の利用可能性

以上のように、この発明では、安全状態にあることを条件に非安全情報を送信するようにしたため、システム稼働中に安全情報（安全信号）以外の情報を安全ネットワークを介して送受信しても、本来の安全情報の応答時間が遅れることがない。

請 求 の 範 囲

1． 安全コントローラと、安全スレーブとが安全ネットワークを介して接続されて構築される安全ネットワークシステムであって、

前記安全スレーブは、安全状態にあるか否かを特定する安全情報を送信する安全情報送信機能と、前記安全情報を含まない非安全情報を送信する非安全情報送信機能を有し、

前記非安全情報送信機能は、前記安全スレーブが安全状態であることを条件に非安全情報を送信するようにしたことを特徴とする安全ネットワークシステム。

2． 前記安全スレーブは、前記非安全情報を送信するタイミングの際に安全でないと判断した場合には、前記非安全情報を送ることなく前記安全を送信するようにしたことを特徴とする請求の範囲第1項に記載の安全ネットワークシステム。

3． 前記安全コントローラは、前記非安全情報を受信した場合には、その非安全情報の送信元の前記安全スレーブは安全状態にあると推定するようにしたことを特徴とする請求の範囲第1項に記載の安全ネットワークシステム。

4． 安全コントローラと、安全スレーブとが安全ネットワークを介して接続されて構築される安全ネットワークシステムに接続するための安全スレーブであって、

安全状態にあるか否かを特定する安全情報を送信する安全情報送信機能と、前記安全情報を含まない非安全情報を送信する非安全情報送信機能を有し、

前記非安全情報送信機能は、安全状態であることを条件に非安全情報を送信するようにしたことを特徴とする安全スレーブ。

5． 受信した前記安全コントローラからの要求が、安全情報の要求か非安全情報の要求かを判断し、

前記安全情報の要求の場合には、安全情報を送信し、

前記非安全情報の要求の場合には、自己が安全状態にあるときは前記非安全情報を送信し、安全状態にないときは安全情報を送信するようにしたことを特徴とする請求の範囲第4項に記載の安全スレーブ。

6． 非安全情報を送信する送信タイミングを制御する非安全情報送信制御手段を設け、

前記送信タイミングの際に、安全状態にあることを条件に前記非安全情報を送信するようにしたことを特徴とする請求の範囲第4項に記載の安全スレーブ。

7． 安全コントローラと、安全スレーブとが安全ネットワークを介して接続されて構築される安全ネットワークシステムに接続するための安全コントローラであって、

前記安全スレーブから受信した安全情報の内容を解析し、安全状態に無いと判断した場合に所定の処理を実行するフェイルセーフ処理機能と、

前記非安全情報を受信した場合には、送信元の前記安全スレーブは安全状態にあると推定する機能を備えたことを特徴とする安全コントローラ。

8． 非安全情報の送信要求を発するタイミングを制御する非安全情報要求制御手段を設けたことを特徴とする請求の範囲第7項に記載の安全コントローラ。

9． 安全コントローラと、安全スレーブとが安全ネットワークを介して接続されて構築される安全ネットワークシステムにおける通信方法であって、

前記安全スレーブは、所定のタイミングで前記安全ネットワークを介して前記安全コントローラに向けて、安全状態にあるか否かを特定する安全情報と、前記安全情報を含まない非安全情報のいずれかの情報を送信する処理を行い、

前記非安全情報を送信する処理は、前記安全スレーブが安全状態であることを条件に行うことを特徴とする通信方法。

１０．　安全コントローラと、安全スレーブとが安全ネットワークを介して接続されて構築される安全ネットワークシステムにおける情報収集方法であって、

前記安全スレーブは、安全状態にあるか否かを特定する安全情報を送信する安全情報送信機能と、前記安全情報を含まない非安全情報を送信する非安全情報送信機能を有し、前記非安全情報送信機能は、前記安全スレーブが安全状態であることを条件に非安全情報を送信するものであり、

前記安全スレーブが、前記安全コントローラに向けて情報を送信するに際し、前記安全情報と前記非安全情報のいずれを送信するかを決定し、次いで、その決定した情報を前記安全ネットワークを介して送信し、

前記安全コントローラは、前記安全ネットワークを介して送られてきた前記安全情報或いは前記非安全情報を受信し、受信した情報が前記非安全情報の場合に、その非安全情報に基づく情報を記憶することを特徴とする安全ネットワークシステムにおける情報収集方法。

１１．　安全コントローラと、安全スレーブとが安全ネットワークを介して接続されて構築される安全ネットワークシステムに対し、モニタ装置をさらに接続して構築されるシステムにおけるモニタ方法であって、

前記安全スレーブは、安全状態にあるか否かを特定する安全情報を送信する安全情報送信機能と、前記安全情報を含まない非安全情報を送信する非安全情報送信機能を有するとともに、前記非安全情報送信機能は、前記安全スレーブが安全状態であることを条件に非安全情報を送信するものであり、

前記モニタ装置は、前記安全スレーブから前記安全コントローラに向けて送信される前記非安全情報を取得し、

その取得した非安全情報を解析し、その非安全情報に基づく情報を記憶することを特徴とするモニタ方法。

図 1

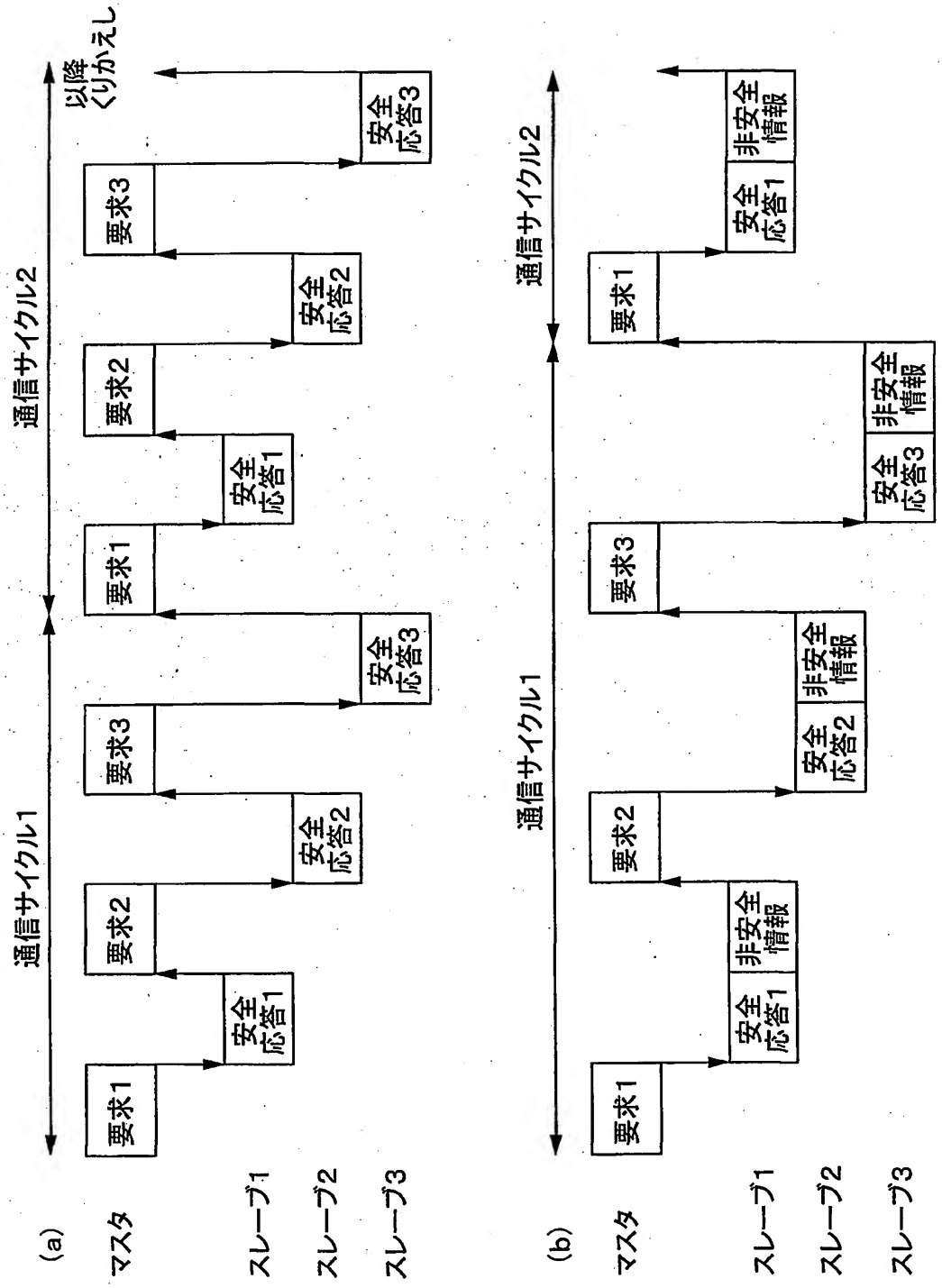

(a)
通信サイクル1
通信サイクル2
以降くりかえし
マスタ
スレーブ1
スレーブ2
スレーブ3
要求1
安全応答1
要求2
安全応答2
要求3
安全応答3
(b)
通信サイクル1
通信サイクル2
非安全情報

図 2

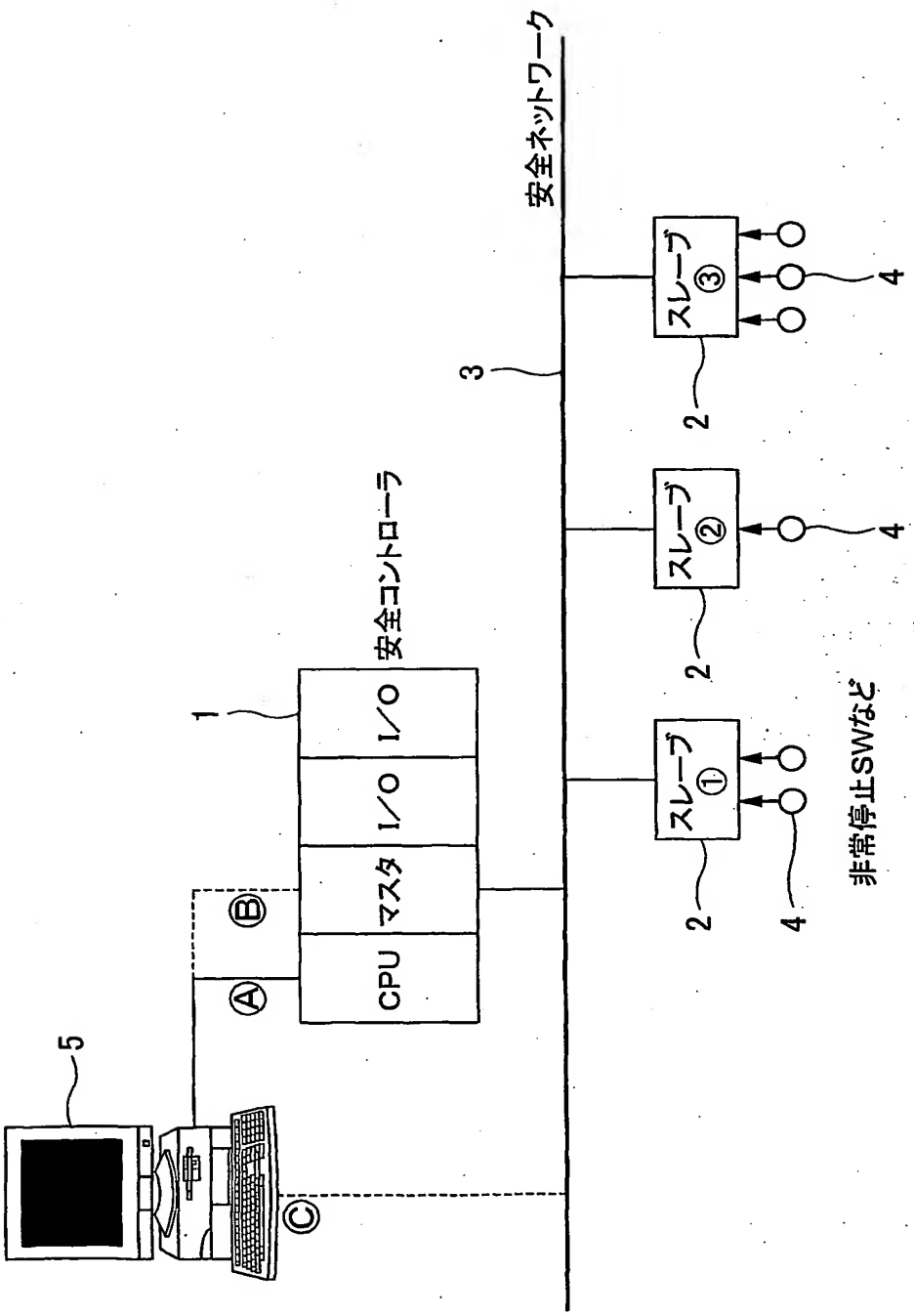

安全ネットワーク
安全コントローラ
CPU
マスタ
I/O
I/O
I/O
Ⓐ
Ⓑ
Ⓒ
スレーブ ①
スレーブ ②
スレーブ ③
非常停止SWなど
1
2
3
4
5

図 3

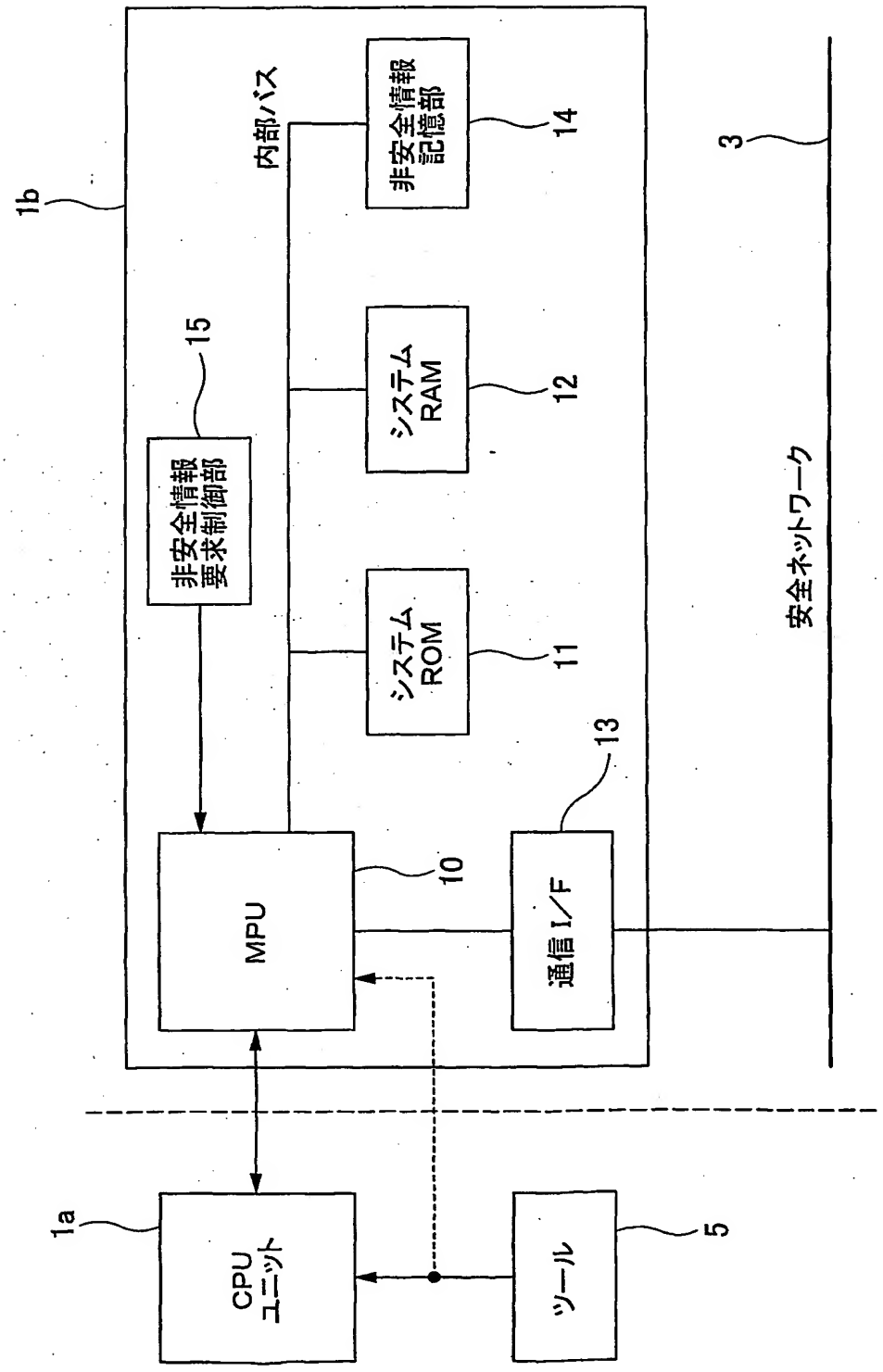

1b
内部バス
非安全情報記憶部
14
3
15
システムRAM
12
非安全情報要求制御部
システムROM
11
安全ネットワーク
13
MPU
10
通信I/F
1a
CPUユニット
ツール
5

図 4

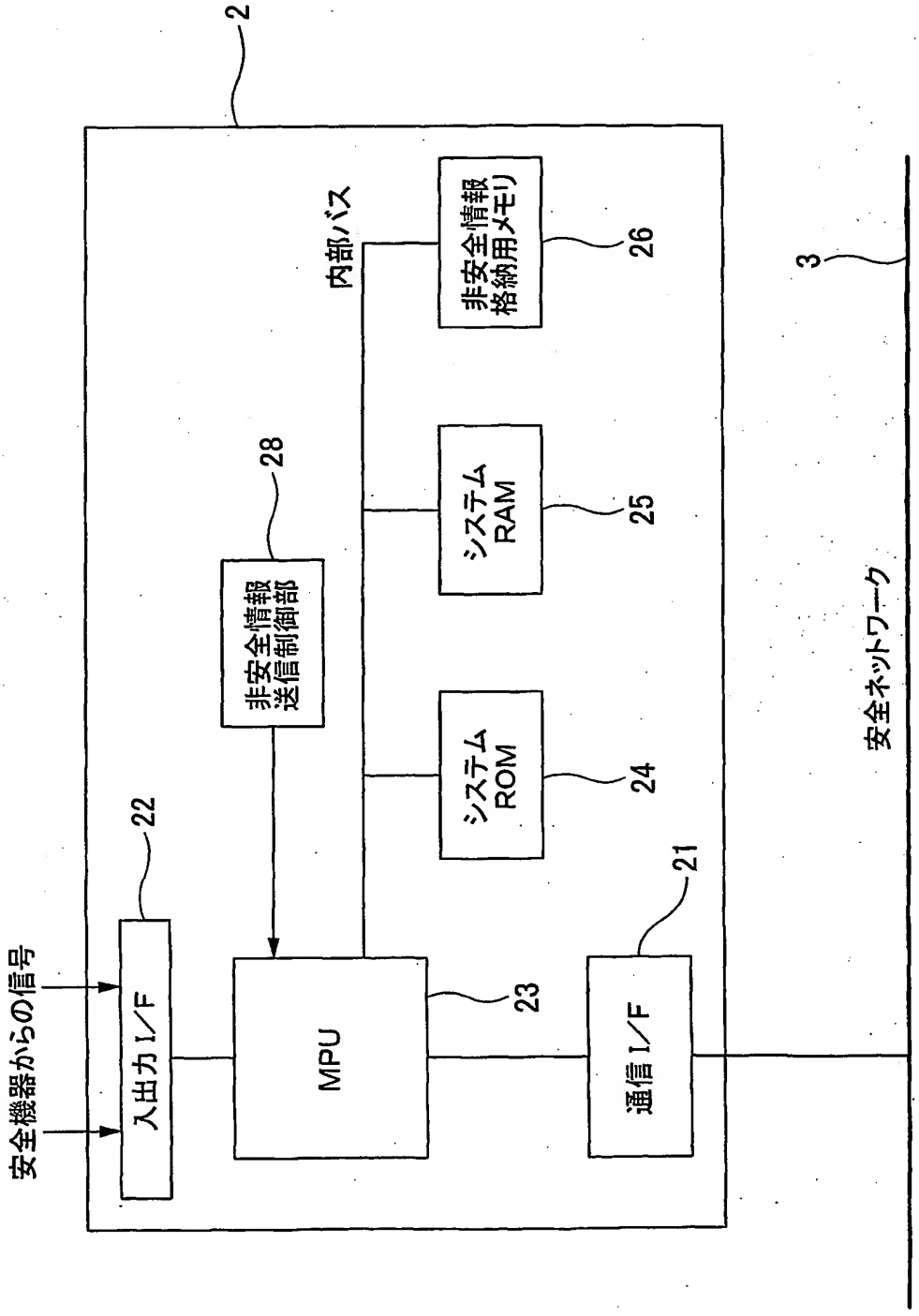

2
内部バス
非安全情報
格納用メモリ
26
3
28
非安全情報
送信制御部
システム
RAM
25
システム
ROM
24
22
21
安全機器からの信号
入出力I/F
MPU
23
通信I/F
安全ネットワーク

図 5

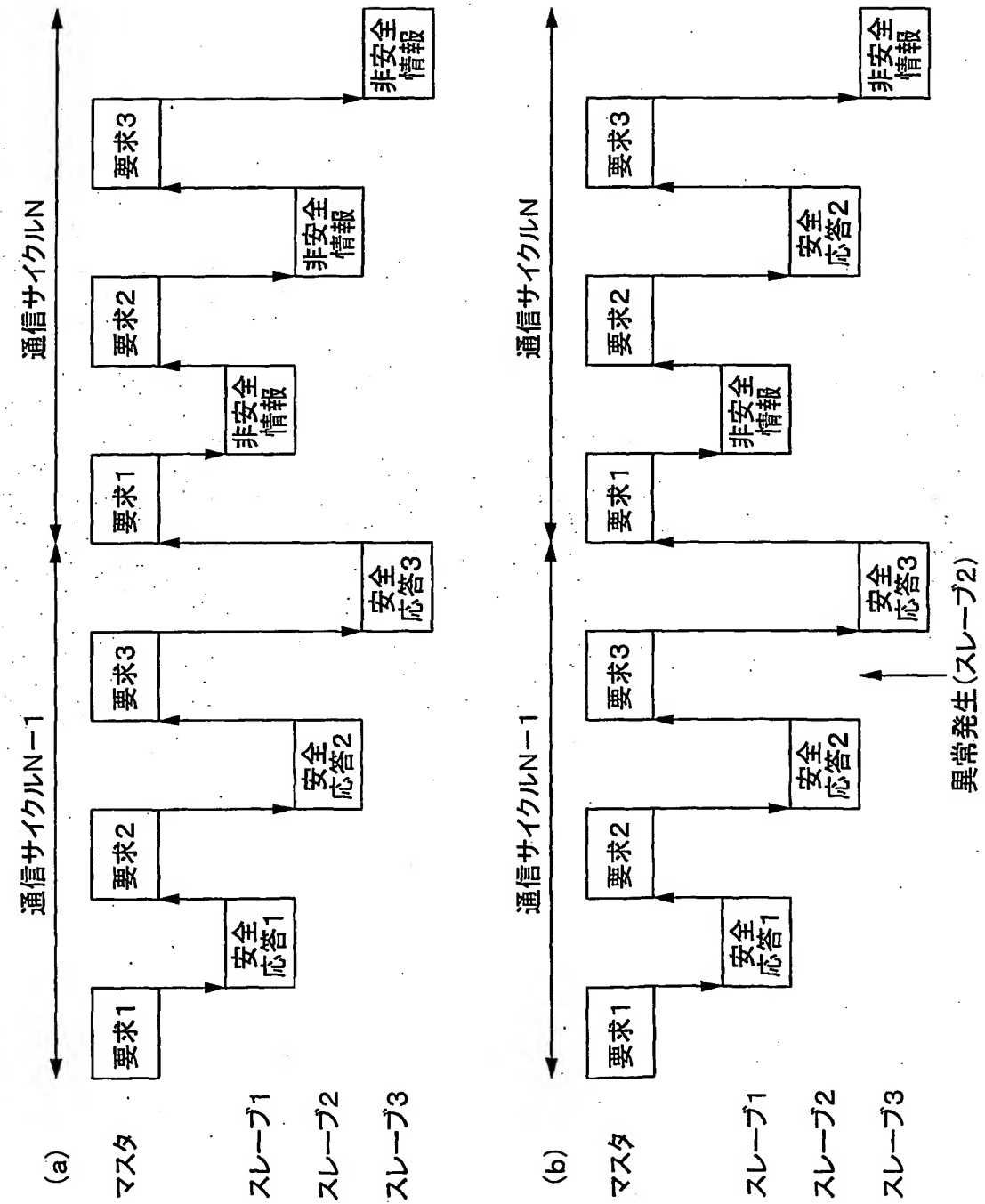

(a)
通信サイクルN−1
通信サイクルN
マスタ
スレーブ1
スレーブ2
スレーブ3
要求1
安全応答1
要求2
安全応答2
要求3
安全応答3
要求1
非安全情報
要求2
非安全情報
要求3
非安全情報
(b)
通信サイクルN−1
通信サイクルN
マスタ
スレーブ1
スレーブ2
スレーブ3
要求1
安全応答1
要求2
安全応答2
要求3
安全応答3
要求1
非安全情報
要求2
安全応答2
要求3
非安全情報
異常発生(スレーブ2)

図 6

シーケンスNo	識別ビット	データ部

識別ビット＝1の時ー安全情報
識別ビット＝0の時ー非安全情報

図 7

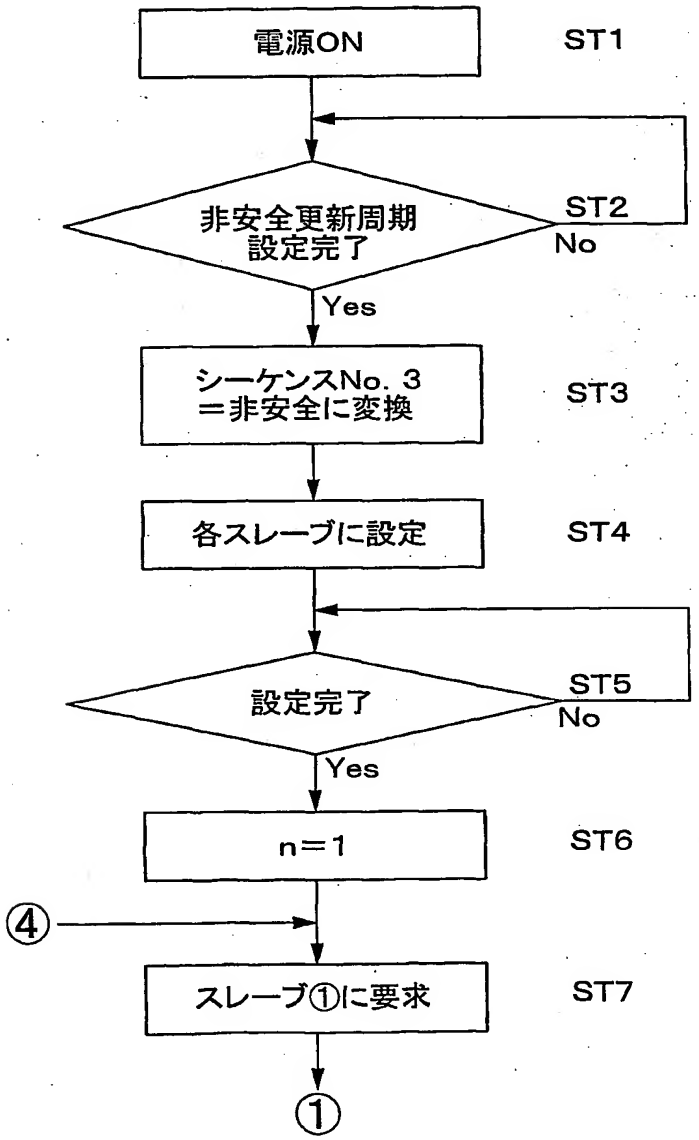


図 8

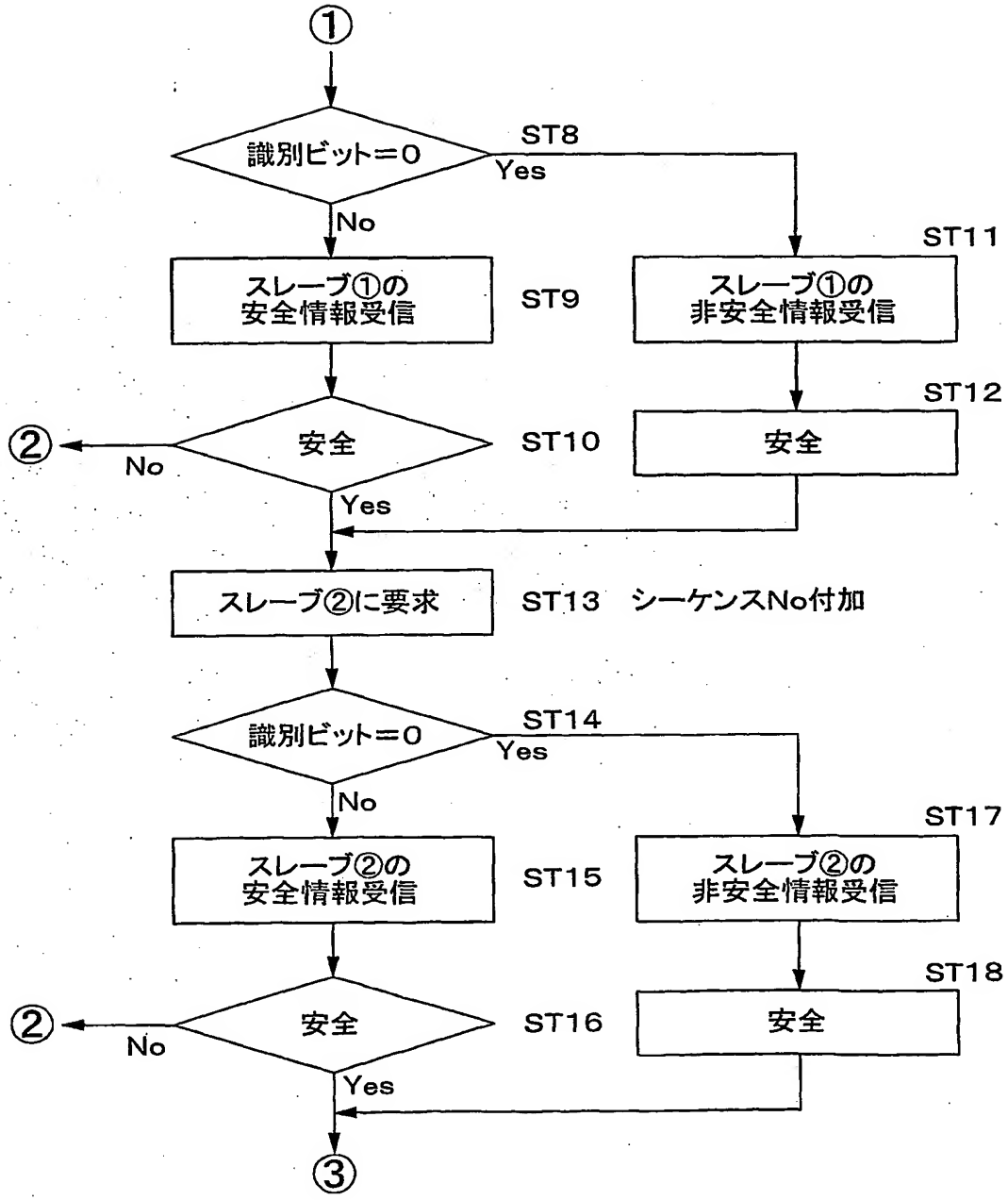

①
識別ビット＝0
ST8
Yes
No
スレーブ①の
安全情報受信
ST9
スレーブ①の
非安全情報受信
ST11
②
No
安全
ST10
安全
ST12
Yes
スレーブ②に要求
ST13 シーケンスNo付加
識別ビット＝0
ST14
Yes
No
スレーブ②の
安全情報受信
ST15
スレーブ②の
非安全情報受信
ST17
②
No
安全
ST16
安全
ST18
Yes
③

図 9

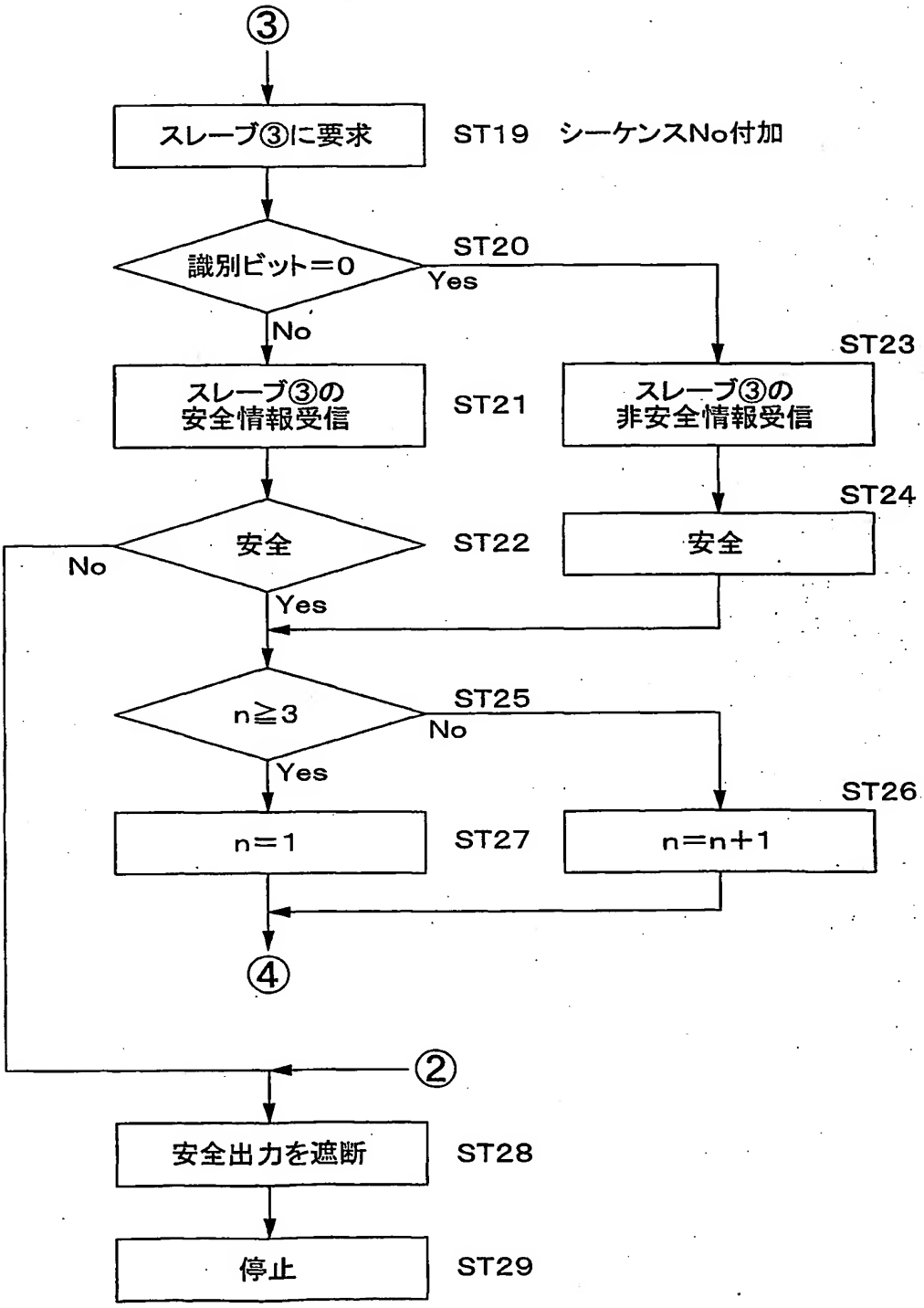

③
スレーブ③に要求
ST19 シーケンスNo付加
識別ビット＝0
ST20
Yes
No
スレーブ③の
安全情報受信
ST21
スレーブ③の
非安全情報受信
ST23
安全
ST22
安全
ST24
No
Yes
n≧3
ST25
No
Yes
n＝1
ST27
n＝n＋1
ST26
④
②
安全出力を遮断
ST28
停止
ST29

図 10

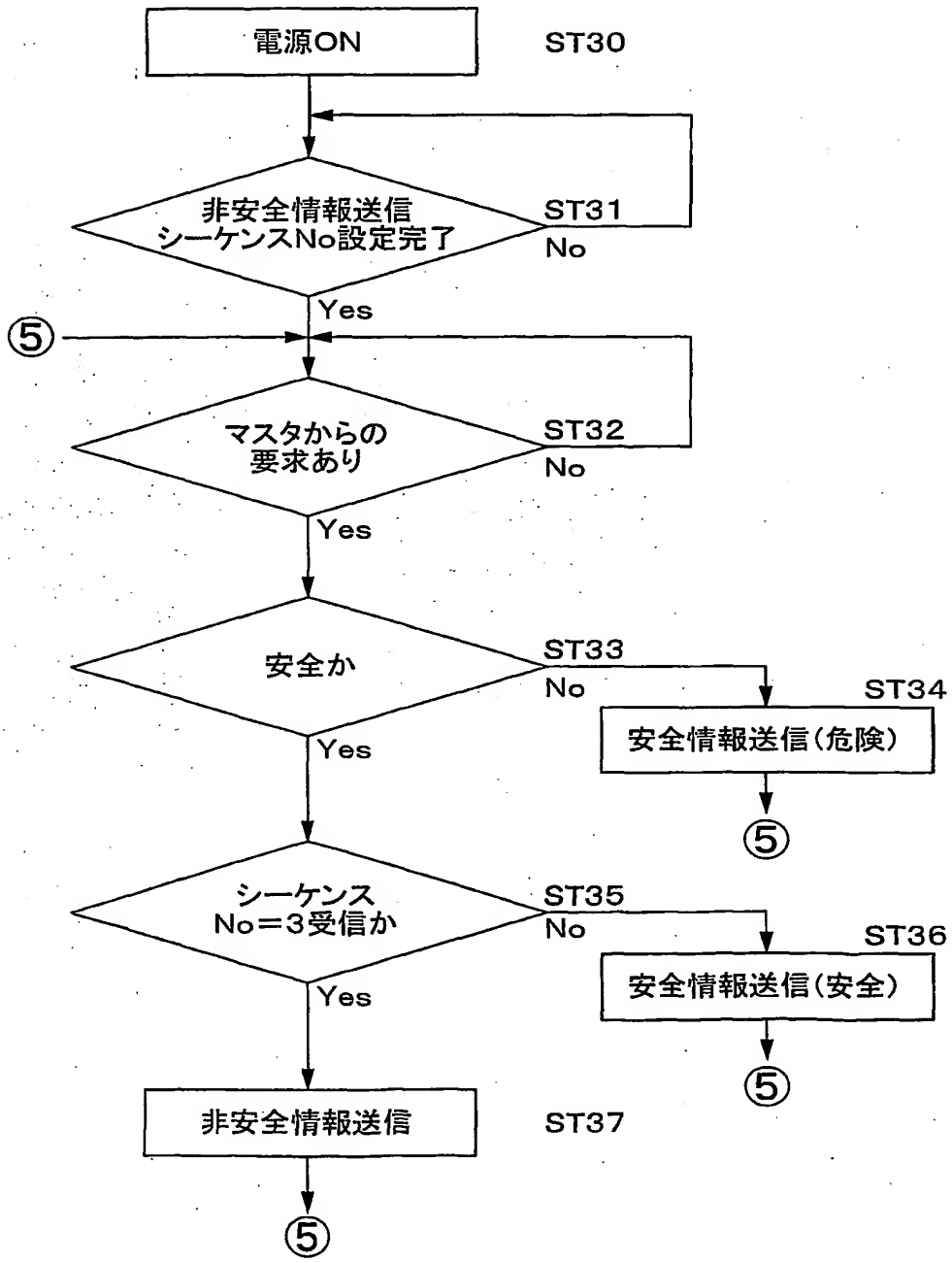

電源ON
ST30
非安全情報送信
シーケンスNo設定完了
ST31
No
Yes
⑤
マスタからの
要求あり
ST32
No
Yes
安全か
ST33
No
ST34
安全情報送信(危険)
⑤
Yes
シーケンス
No＝3受信か
ST35
No
ST36
安全情報送信(安全)
⑤
Yes
非安全情報送信
ST37
⑤

図 11

(a)

シーケンスNo (マスタ送信)	1	2	3	1	2	3	1	2
安全OKの場合	安全OK							
スレーブの送信データ	安全応答	安全応答	非安全情報	安全応答	安全応答	非安全情報	安全応答	安全応答
識別ビット (スレーブが付加)	1	1	0	1	1	0	1	1
マスタの安全確認	安全	安全	安全	安全	安全	安全	安全	安全
マスタ非安全情報	なし	なし	受信	なし	なし	受信	なし	なし

(b)

シーケンスNo (マスタ送信)	1	2	3	1	2	3
安全NGの場合	安全OK			安全NG		
スレーブの送信データ	安全応答	安全応答	非安全情報	安全応答	安全応答	安全応答
識別ビット (スレーブが付加)	1	1	0	1	1	1
マスタの安全確認	安全	安全	安全	安全	安全	危険
マスタ非安全情報	なし	なし	受信	なし	なし	なし

図 12

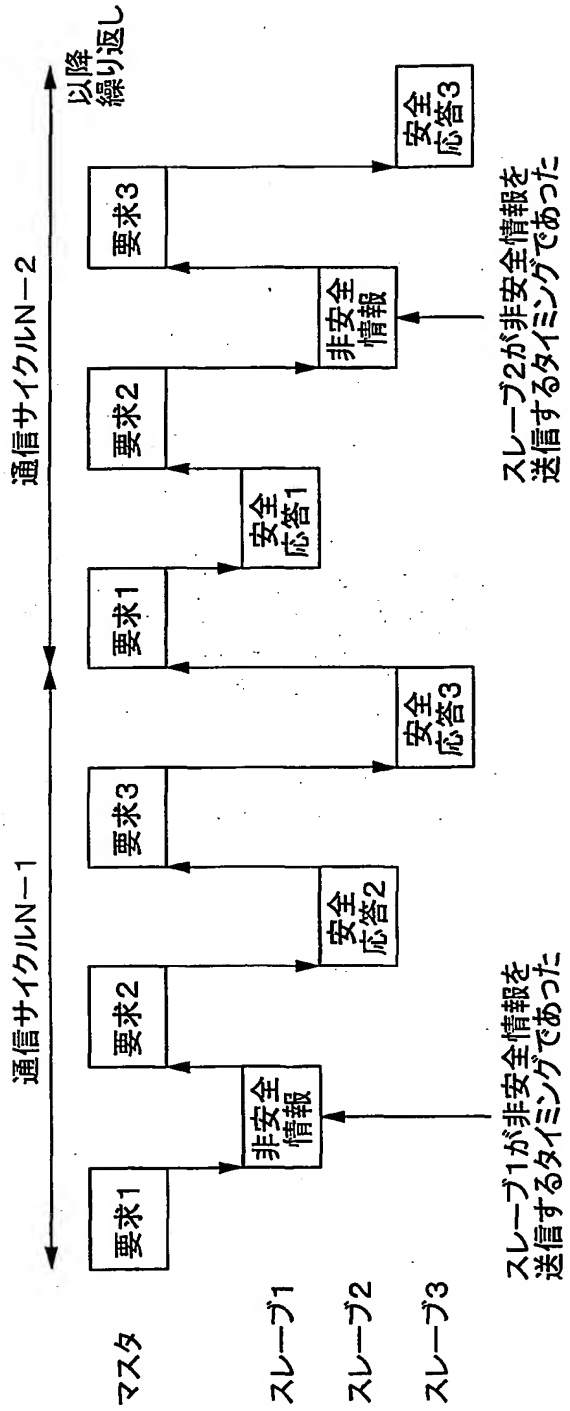

以降
繰り返し
通信サイクルN−2
通信サイクルN−1
要求1
非安全
情報
要求2
安全
応答2
要求3
安全
応答3
要求1
安全
応答1
要求2
非安全
情報
要求3
安全
応答3
マスタ
スレーブ1
スレーブ2
スレーブ3
スレーブ1が非安全情報を
送信するタイミングであった
スレーブ2が非安全情報を
送信するタイミングであった

図 13

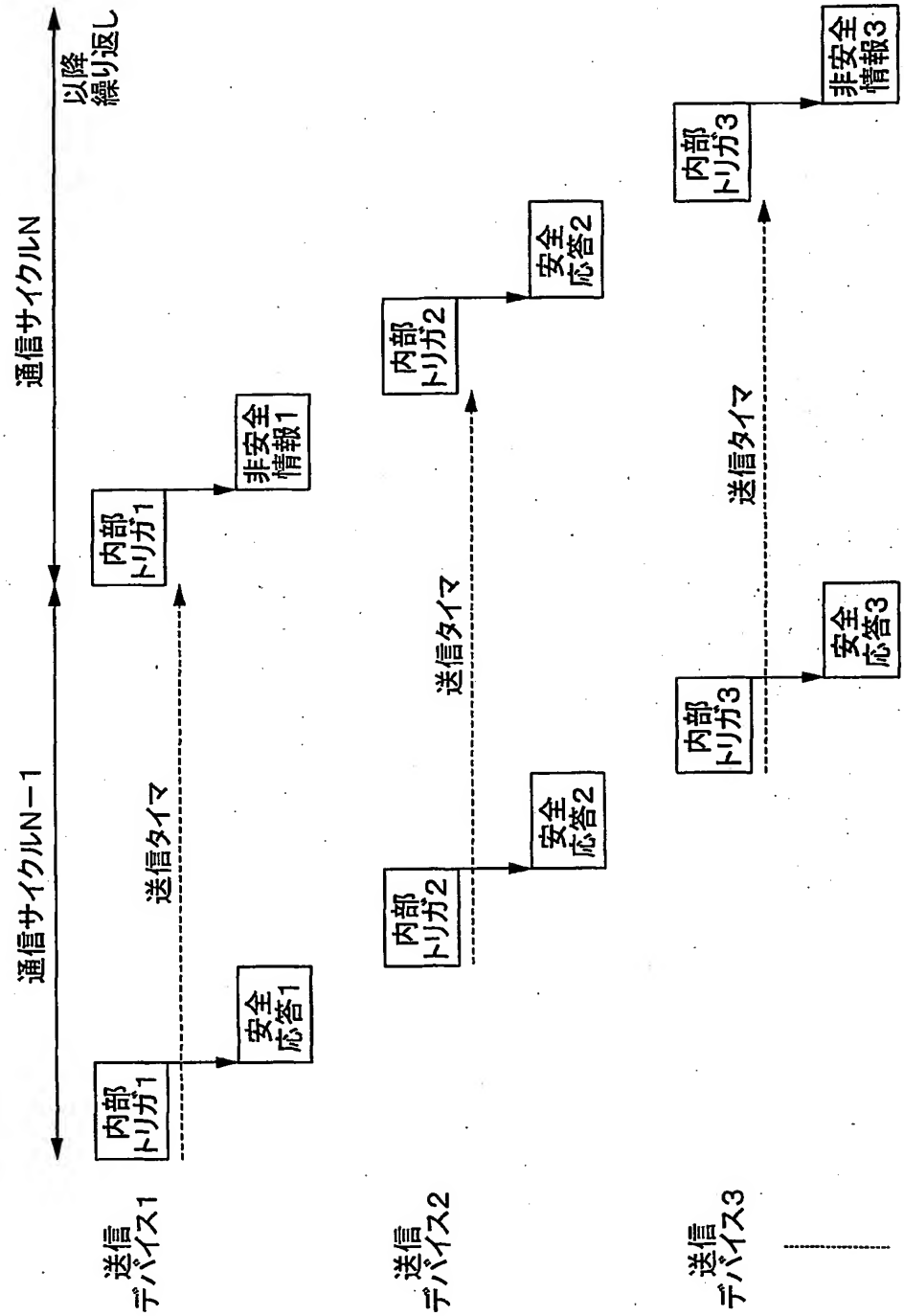

通信サイクルN−1
通信サイクルN
以降
繰り返し
送信
デバイス1
内部
トリガ1
送信タイマ
安全
応答1
内部
トリガ1
非安全
情報1
送信
デバイス2
内部
トリガ2
送信タイマ
安全
応答2
内部
トリガ2
安全
応答2
送信
デバイス3
内部
トリガ3
送信タイマ
安全
応答3
内部
トリガ3
非安全
情報3

図 14

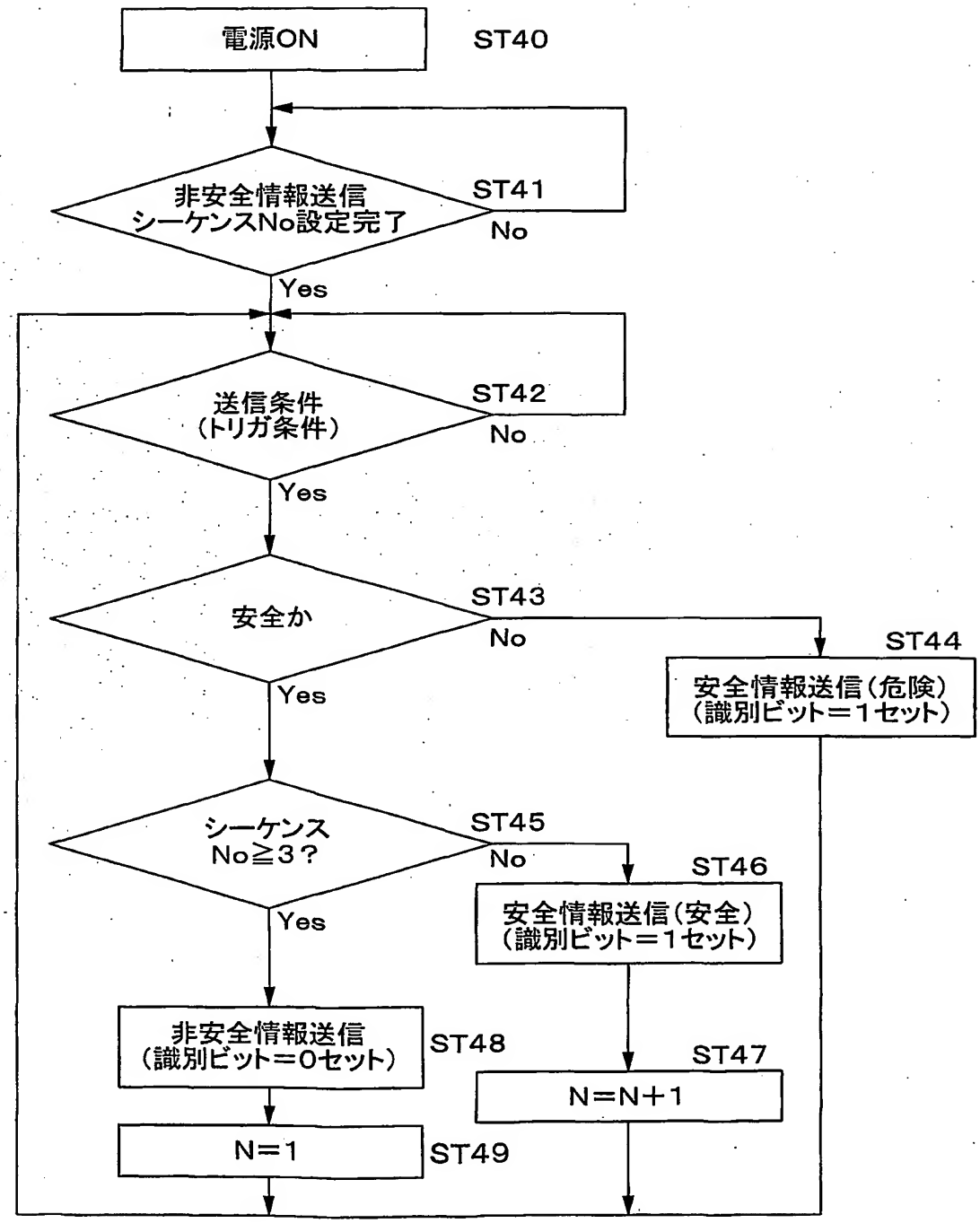

電源ON
ST40
非安全情報送信
シーケンスNo設定完了
ST41
No
Yes
送信条件
(トリガ条件)
ST42
No
Yes
安全か
ST43
No
ST44
安全情報送信(危険)
(識別ビット＝1セット)
Yes
シーケンス
No≧3？
ST45
No
ST46
安全情報送信(安全)
(識別ビット＝1セット)
Yes
非安全情報送信
(識別ビット＝0セット)
ST48
ST47
N＝N＋1
N＝1
ST49

図 15

送信側アドレス	識別ビット	データ部

識別ビット＝1の時ー安全情報
識別ビット＝0の時ー非安全情報

図 16